

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Rachel S. Corn, a Special Agent (SA) with the Federal Bureau of Investigation (FBI), Baltimore Division, Baltimore, Maryland, being duly sworn, depose and state as follows:

1. I have been a SA with the FBI since May 2006. Since September 2006, I have primarily investigated federal violations concerning child pornography and the sexual exploitation of children. I have gained experience through training in seminars, classes, and daily work related to conducting these types of investigations. Specifically, I have received FBI Crimes Against Children training, FBI Innocent Images Online Undercover training, and FBI Peer-to-Peer Network Online Investigation training. I have participated in the execution of numerous search warrants, of which the majority have involved child exploitation and/or child pornography offenses. Many of the child exploitation and/or child pornography search warrants resulted in the seizure of computers, cell phones, magnetic storage media for computers, other electronic media, and other items evidencing violations of federal laws, including various sections of Title 18, United States Code § 2252A involving child exploitation offenses. I have also participated in the execution of numerous search warrants for online accounts, such as email accounts, online storage accounts and other online communication accounts related to child exploitation and/or child pornography. In the course of my employment with the FBI, I have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media and within online accounts.

2. As a federal agent, I am authorized to investigate violations of laws of the United States and am a law enforcement officer with the authority to execute warrants issued under the authority of the United States.

3. This affidavit is made in support of an application for a warrant to search the following (hereinafter referred to as the “TARGET ACCOUNTS and REPORTS”):

a. The Twitter accounts associated with:

1. lslow7776@gmail.com and Username: AxlJonez;
2. lslow77666@gmail.com and Username: baitsgalore;
3. robotkid143@gmail.com and Username: boyzbait;
4. lslow5566@gmail.com and Username: boyzgalore;
5. lslow7766@gmail.com and Username: boyzheaven1;
6. mariasmith77666@gmail.com and Username: DallasBait;
7. lslow2233@gmail.com and Username: GriffinLuv1;
8. lslow6677@gmail.com and Username: heavenlyguys1;
9. lslow222333@gmail.com and Username: JaxxGriffin;
10. linaslow9988@gmail.com and Username: KellarHeart;
11. msmithz2233@gmail.com and Username: KingTKworld;
12. ryankeely1122@gmail.com and Username: lina54592483;
13. lslow8877@gmail.com and Username: BraxJonez;
14. lslow2334@gmail.com and Username: BraxDamon;
15. phoebekay132@gmail.com and Username: BraxDiamond;
16. Username: BraxLucas;
17. kaylacole7766@gmail.com and Username: CamEvanzz;
18. mkay3973@gmail.com and Username: Marieka38187058;
19. mariasmith12122@gmail.com and Username: AxlDeen;
20. phone number 2035204961 and Username: FinnJaxen;

21. phone number 2035204961 and Username: LilySlos; and
22. phone number 2035204961 and Whateve18718239;

b. The associated files of Cybertipline Reports 90692565, 90693502, 90693602, and 90693794, that were forwarded to the National Center for Missing and Exploited Children (NCMEC) by Twitter, Inc.

4. The TARGET ACCOUNTS and REPORTS are to be searched for evidence of violations of Title 18, United States Code, Sections 2251(a) (sexual exploitation of children); Title 18, United States Code, Section 2252A(a)(2) (distribution and receipt of child pornography); Title 18, United States Code, Section 2252A(a)(5)(B) (possession of child pornography); Title 18 United States Code, Section 2261A(2)(b)(cyberstalking); and Title 18 United States Code, Section 2242(b)(coercion and enticement) (the “TARGET OFFENSES”).

5. The statements in this affidavit are based in part on information and reports provided by the Baltimore City Police Department, the Noblesville Police Department, located in Noblesville, Indiana, on my investigation of this matter, and on my experience and background as a Special Agent of the FBI. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the TARGET OFFENSES are located in the TARGET ACCOUNTS and REPORTS.

SUMMARY CONCERNING CHILD PORNOGRAPHY, PERSONS WHO POSSESS AND COLLECT CHILD PORNOGRAPHY AND HOW USE OF COMPUTERS AND THE INTERNET RELATES TO THE POSSESSION, RECEIPT AND DISTRIBUTION OF CHILD PORNOGRAPHY

6. Based on my investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned that individuals who utilize the internet to view and receive images of

child pornography are often individuals who have a sexual interest in children and in images of children, and that there are certain characteristics common to such individuals, including the following:

a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children or images of children frequently maintain their “hard copies” of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, individuals who have a sexual interest in children or images of children often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer or cellphone, and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector’s residence, or in online storage, email accounts or other online communication accounts, to enable the individual to view the collection, which is valued highly.

e. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/collectors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography. This data is typically in digital format, and often maintained on computers, cell phones and in online storage, email accounts or other online communication accounts.

f. Individuals who would have knowledge on how to distribute and receive digital images of child pornography through the use of Peer to Peer networks and other online

methods would have gained knowledge of its location through online communication with others of similar interest. Other forums, such as bulletin boards, newsgroups, IRC chat or chat rooms have forums dedicated to the trafficking of child pornography images. Individuals who utilize these types of forums are considered more advanced users and therefore more experienced in acquiring a collection of child pornography images.

g. Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged time period. This behavior has been consistently documented by law enforcement officers involved in the investigation of child pornography.

7. Based on my investigative experience related to computer and internet related child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned the following:

a. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies.) The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.

b. The development of computers, smartphones and the internet have added to the methods used by child pornography collectors to interact with and sexually exploit children. Computers, smartphones and the internet serve four functions in connection with child pornography. These are production, communication, distribution, and storage.

c. Mobile devices such as laptop computers, smartphones, iPods, iPads and digital media storage devices are known to be used and stored in vehicles, on persons or other areas outside of the residence.

d. Smartphones have the capability to access the Internet and store information, such as videos and images. As a result, an individual using a smartphone can send, receive, and store files, including child pornography, without accessing a personal computer or laptop. An individual using a smartphone can also easily plug the device into a computer, via a USB cable, and transfer data files from one digital device to another. Many people generally carry their smartphone on their person.

e. Child pornographers can now transfer photographs from a camera onto a computer-readable format. With the advent of digital cameras, the images can now be transferred directly onto a computer. A device known as a modem allows any computer to connect to another

computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography.

f. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., “Instant Messaging”), easy access to the Internet, and online file sharing and storage, the computer is a preferred method of distribution and receipt of child pornographic materials.

g. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion. Collectors and distributors of child pornography use online resources to retrieve and store child pornography, including services offered by Internet Portals such as AOL Inc., Yahoo, and Google, Inc., Facebook, Dropbox, Instagram, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services, file exchange services, messaging services, as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Email accounts, online storage accounts, and other online communication accounts allow users to save significant amounts of data, including email, images, videos, and other files. The data is maintained on the servers of the providers, and is occasionally retained by the providers after the user deletes the data from their account.

h. In my recent investigative experience, as well as recent discussions with law enforcement officers, I know that individuals who collect child pornography are using email accounts, online storage accounts, and other online communications accounts to obtain, store, maintain, and trade child pornography with growing frequency, in addition to, or as an alternative to, the use of personal devices.

i. Based on traits shared by collectors, the use of email, online storage accounts, and other online communication accounts, and the increased storage capacity of computers and server space over time, there exists a fair probability that evidence regarding the distribution, receipt and possession of child pornography will be found in the TARGET ACCOUNTS and REPORTS notwithstanding the passage of time.

j. In addition, computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they may be recoverable months or years later using readily available forensic tools.

k. When a person “deletes” a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or

slack space that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space for long periods of time before they are overwritten.

l. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages.

m. The storage capacity of personal computers has increased dramatically over the last few years. Common and commercially available hard drives are now capable of storing over 500 GB of data. With that amount of storage space, an individual could store thousands of video files and/or hundreds of thousands of image files.

n. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Since the storage capacity of hard drives has increased dramatically over the last several years, it is more likely that the above-described information will be recovered during forensic analysis.

NCMEC CYBERTIPLINE

8. The National Center for Missing and Exploited Children (NCMEC) receives complaints via their Cybertipline from Internet Service Providers (ISPs), Electronic Service Providers (ESPs), and others. These Cybertipline reports are reviewed by a NCMEC analyst and forwarded to law enforcement for further investigation on the information provided in the Cybertipline report.

TWITTER

9. Twitter is a microblogging and social networking service where users can communicate with others through the exchange of quick, frequent messages. Users post and interact with messages known as "tweets." Tweets may contain photos, videos, links, and text. Users can send Direct Messages to have private conversations with other users. In addition to text, you can include a photo, video, or GIF via Direct Message.

PROBABLE CAUSE

10. In December 2019, a minor male, born in 2002, advised that after sending sexually explicit videos and images to the user of the Instagram account associated with lslow7766@gmail.com (“Linamarie6.5”) and User ID: 10895080946, and Snapchat account lslow6_5, the user requested the minor to send additional specific images and if he refused, the user would forward the initial sexually explicit files to the minor’s friends and family.

11. In April 2020, another minor male, born in 2006, advised that after sending sexually explicit videos and images to the user of the Instagram account associated with lslow6655@gmail.com (“Linamarie6.7”) and User ID: 18314925887, and Snapchat account lslow6_5, the user requested the minor to send additional specific files and if he refused, the user would forward the initial sexually explicit files to the minor’s friends and family.

12. On December 16, 2020, United States Magistrate Judge Thomas M. DiGirolamo, of the District of Maryland, granted search warrants, which were executed the same day, for numerous Google, Facebook, Instagram, Snapchat, Apple, Dropbox, Kik, TextNow, Pornhub, Oath, and the following Twitter accounts¹:

1. <https://twitter.com/Thirstyforsaus1/status/1233203087419924484>;
2. User ID: @Thirstyforsaus1;
3. lslow7776@gmail.com;
4. lslow77666@gmail.com;
5. robotkid143@gmail.com;
6. lslow5566@gmail.com;
7. lslow7766@gmail.com;
8. mariasmith77666@gmail.com;
9. lslow2233@gmail.com;
10. lslow6677@gmail.com;
11. lslow222333@gmail.com;
12. linaslow9988@gmail.com;
13. msmithz2233@gmail.com;
14. ryankeely1122@gmail.com;
15. lslow8877@gmail.com; and
16. mkwalsh2015@aol.com;

¹ The Twitter search warrant did not request Twitter to provide Direct Messages. This search warrant is requesting Twitter to provide Direct Messages associated with the 13 of these accounts (#s 3-15).

13. On April 20, 2021, United States Magistrate Judge Thomas M. DiGirolamo, of the District of Maryland, granted search warrants for several Google, Instagram, and Snapchat accounts, and the residence, person and vehicle of Matthew Keith Walsh (“Walsh”). The residential search warrant was executed on April 21, 2021. A cell phone and laptop were seized and are still being forensically examined.

14. Walsh, born in 1997, was present during the execution of the residential search warrant and waived his Miranda rights and consented to an interview, in which I participated in, and which was audio recorded. Walsh advised that his cell phone number was **203-520-4961** and that no one else used his cell phone or laptop, which were both password protected. Walsh admitted to “catfishing” which he explained was posing as another person online. Walsh was catfishing by pretending to be a female named “Lina” online. Walsh said he met minors on Instagram and asked them for sexually explicit files and the minors sent the files. If the minors did not want to send the sexually explicit files anymore, Walsh told the minors that they either send him the files or Walsh would post the minors’ nudes online or send them to the minors’ families. Walsh said that he was not really going to “expose” the minors. Walsh explained that he sent the nudes to the minors’ friends on Instagram, took a screenshot, then unsent the message before the friend saw the nudes. Walsh said he communicated with 14 to 17 years old and that he estimated that he received pictures from 50 minors and blackmailed 25 of them. Walsh explained that he did not blackmail all of the minors because he did not need to because those minors continued to send pictures to Walsh.

15. Walsh stated he sold the pornography he obtained from the minors using **Twitter**. Walsh did not tell the people he sold the pornography to that it was of minors. People paid Walsh through PayPal, Venmo and Cash App. Walsh provided people his payment information through

messages on **Twitter**. Walsh sent the people a Mega² link through **Twitter** and then deleted the link after the people saved the files. Walsh stated that he made \$8000 from selling the minors' files. The minors did not know their pictures were on **Twitter** or that Walsh sold their pictures. When asked if Walsh did this for money, Walsh said no, he did it because he was bored and horny.

16. Walsh stated he saved the pornography from the minors he received in his Mega account. Walsh said he saved the files into folders of fake names or a variation of the person's real name. Walsh provided consent to search his Mega account. In the Mega account there are folders with various names containing sexually explicit files of numerous males. Many of the files saved on Mega have the following Twitter usernames written on them: **@BraxJones**, **@BraxDamon**, **@BraxLucas**, and **@CamEvanzz**.

17. Throughout the investigation, Google has provided various responses to search warrants and court orders. Google responses include documents titled "Accounts Linked By Cookies" and "Accounts Linked By Creation IP Addresses." Within those documents, these additional email addresses were linked to other accounts found to be created, controlled, or used by Walsh:

lslow2334@gmail.com,
phoebekay132@gmail.com
kaylacole7766@gmail.com
mkay3973@gmail.com
mariasmith12122@gmail.com

18. On May 12, 2021, a grand jury sitting in the district of Maryland returned a six-count indictment charging Matthew Keith Walsh with Sexual Exploitation of a Minor, Coercion and Enticement, and Receipt of Child Pornography. (United States v. Matthew Keith Walsh, ELH-21-0161). On May 14, 2021, Walsh was arrested and has been detained since that time.

² Mega is a cloud storage and file hosting service that can be accessed through a website or an app on your mobile device.

19. On May 21, 2021, **Twitter** sent **Cybertipline Report 90692565** to NCMEC and listed the Incident Types as “Child Pornography (possession, manufacture, and distribution).” The report for 90692565 stated that the Incident Time was 07/30/2020. Twitter listed the “suspect” account username **BraxDiamond** and stated “User appears to have engaged in apparent child sexual exploitation activity.” Twitter provided two files with the report. In the Cybertipline Report, Twitter did not provide information on whether they had reviewed one of the two files associated with the Cybertipline report.

20. On May 21, 2021, **Twitter** sent **Cybertipline Report 90693502** to NCMEC and listed the Incident Types as “Child Pornography (possession, manufacture, and distribution).” The report for 90693502 stated that the Incident Time was 06/11/2020. Twitter listed the “suspect” account username **BraxDamon** and stated “User appears to have engaged in apparent child sexual exploitation activity.” Twitter provided two files with the report. In the Cybertipline Report, Twitter did not provide information on whether they had reviewed one of the two files associated with the Cybertipline report.







21. On May 21, 2021, **Twitter** sent **Cybertipline Report 90693602** to NCMEC and listed the Incident Types as “Child Pornography (possession, manufacture, and distribution).” The report for 90693602 stated that the Incident Time was 09/11/2018. Twitter listed the “suspect” account username **BraxLucas** and stated “User appears to have engaged in apparent child sexual exploitation activity.” Twitter provided one file with the report. In the Cybertipline Report, Twitter did not provide information on whether they had reviewed the one file associated with the Cybertipline report.




22. On May 21, 2021, **Twitter** sent **Cybertipline Report 90693794** to NCMEC and listed the Incident Types as “Child Pornography (possession, manufacture, and distribution).” The

report for 90693794 stated that the Incident Time was 12/12/2019. Twitter listed the “suspect” account username **CamEvanzz** and stated “User appears to have engaged in apparent child sexual exploitation activity.” Twitter provided two files with the report. In the Cybertipline Report, Twitter did not provide information on whether they had reviewed one of the two files associated with the Cybertipline report.

TARGET ACCOUNTS



23. **Twitter** provided the following information in response to administrative subpoenas for the following accounts:

- | | |
|----|--|
| a. | Username: AxlJonez
Display Name:  AxlJonez 
Email: lslow7776@gmail.com
Created Date: 08/22/2019
Creation IP: 73.163.147.2
Phone Number: 203-520-4961 |
| b. | Username: baitsgalore
Display Name:  baitsgalore 
Email: lslow77666@gmail.com
Created Date: 06/06/2019
Creation IP: 73.163.147.2 |
| c. | Username: boyzbait
Display Name: boyzbait
Email: robotkid143@gmail.com
Created Date: 08/24/2019
Creation IP: 199.167.137.17 |
| d. | Username: boyzgalore
Display Name:  boyzgalore 
Email: lslow5566@gmail.com
Created Date: 07/17/2019
Creation IP: 73.163.147.2
Phone Number: 970-648-4091 |
| e. | Username: boyzheaven1
Display Name: b
Email: lslow7766@gmail.com
Created Date: 04/19/2019 |

- Creation IP: 75.102.135.228
- f. Username: **DallasBait**
 Display Name: Dallasbaits 
 Email: **mariasmith77666@gmail.com**
 Created Date: 02/08/2020
 Creation IP: 45.56.142.125
 Phone Number: 239-284-4207³
- g. Username: **GriffinLuv1**
 Display Name: ♡ GriffinLuv ♡
 Email: **lslow2233@gmail.com**
 Created Date: 09/02/2019
 Creation IP: 71.19.252.144
 Phone Number: 203-520-0031
- h. Username: **heavenlyguys1**
 Display Name: heavenlyguys
 Email: **lslow6677@gmail.com**
 Created Date: 07/16/2019
 Creation IP: 73.163.147.2
- i. Username: **JaxxGriffin**
 Display Name:  JaxxGriffin 
 Email: **lslow222333@gmail.com**
 Created Date: 08/24/2019
 Creation IP: 199.167.137.98
 Phone Number: 970-648-4091
- j. Username: **KellarHeart**
 Display Name: Kellar Heart ♡
 Email: **linaslow9988@gmail.com**
 Created Date: 10/06/2019
 Creation IP: 104.237.80.82
 Phone Number: 203-520-4961
- k. Username: **KingTKworld**
 Display Name: King TK
 Email: **msmithz2233@gmail.com**
 Created Date: 09/01/2019
 Creation IP: 172.102.228.158
 Phone Number: 705-994-2878

³ An administrative subpoena was sent to Verizon for the phone number 239-284-4207. Verizon provided the subscriber information for the account as Kimberly Robbins, 3937 Aquilla Drive, Lakeland, Florida, contact name: Jakob Robbins.

- l. Username: **lina54592483**
Display Name: lina
Email: **ryankeely1122@gmail.com**
Created Date: 11/01/2019
Creation IP: 73.163.147.2
- m. Username: **BraxJonez**
Display Name: Brax jonez
Email: **lslow8877@gmail.com**
Created Date: 05/08/2020
Creation IP: 73.163.147.2
Phone Number: 2035204961
- n. Username: **BraxDamon**
Display Name: Brax Damon
Email: **lslow2334@gmail.com**
Created Date: 06/11/2020
Creation IP: 73.163.147.2
Phone Number: 4102416994
- o. Username: **BraxDiamond**
Display Name: Brax Diamond
Email: **phoebekay132@gmail.com**
Created Date: 07/30/2020
Creation IP: 73.163.147.2
Phone Number: 4109247998
- p. Username: **BraxLucas**
Display Name: LucasBrax
Created Date: 09/11/2018
Phone Number: 5562982515103
- q. Username: **CamEvanzz**
Display Name: Cam Evanz
Email: **kaylacole7766@gmail.com**
Created Date: 12/12/2019
Creation IP: 104.238.46.173
Phone Number: 4436026241
- r. Username: **Marieka38187058**
Display Name: marie kay
Email: **mkay3973@gmail.com**
Created Date: 03/26/2021
Creation IP: 73.172.240.95
- s. Username: **AxlDeen**

	Display Name:	 AxlDeen 
	Email:	mariasmith12122@gmail.com
	Created Date:	08/24/2019
	Creation IP:	73.163.147.2
	Phone Number:	2035204961
t.	Username:	FinnJaxen
	Display Name:	axeljames
	Phone Number:	2035204961
	Created Date:	09/28/2019
	Creation IP:	104.238.59.92
u.	Username:	LilySlos
	Display Name:	lily slos
	Phone Number:	2035204961
	Created Date:	01/19/2020
	Creation IP:	174.205.3.73
v.	Username:	Whateve18718239
	Display Name:	whatever
	Phone Number:	2035204961
	Created Date:	01/02/2020
	Creation IP:	174.205.12.38

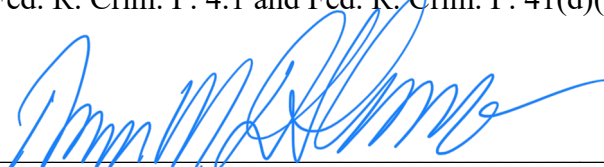
CONCLUSION

24. Based on the foregoing information, I have probable cause to believe that contraband, evidence, fruits, and instrumentalities of the TARGET OFFENSES as set forth herein and in Attachments B1 and B2, are currently contained in the TARGET ACCOUNTS and REPORTS, more fully described in Attachments A1 and A2. I therefore respectfully request that search warrants be issued authorizing the search of the accounts described in Attachments A1 and A2, for the items described in Attachments B1 and B2, and authorizing the seizure and examination of any such items found therein.

Rachel S Corn

 Special Agent Rachel S. Corn
 Federal Bureau of Investigation

Affidavit submitted by email and attested to me as true and accurate by telephone consistent with Fed. R. Crim. P. 4.1 and Fed. R. Crim. P. 41(d)(3) this 30 day of June, 2021.



HONORABLE THOMAS M. DIGIROLAMO
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A1 - Twitter, Inc

This warrant applies to information associated with the following Twitter, Inc., accounts associated with the following:

- lslow7776@gmail.com and Username: AxlJonez;
- lslow77666@gmail.com and Username: baitsgalore;
- robotkid143@gmail.com and Username: boyzbait;
- lslow5566@gmail.com and Username: boyzgalore;
- lslow7766@gmail.com and Username: boyzheaven1;
- mariasmith77666@gmail.com and Username: DallasBait;
- lslow2233@gmail.com and Username: GriffinLuv1;
- lslow6677@gmail.com and Username: heavenlyguys1;
- lslow222333@gmail.com and Username: JaxxGriffin;
- linaslow9988@gmail.com and Username: KellarHeart;
- msmithz2233@gmail.com and Username: KingTKworld;
- ryankeely1122@gmail.com and Username: lina54592483;
- lslow8877@gmail.com and Username: BraxJonez;
- lslow2334@gmail.com and Username: BraxDamon;
- phoebekay132@gmail.com and Username: BraxDiamond;
- Username: BraxLucas;
- kaylacole7766@gmail.com and Username: CamEvanzz;
- mkay3973@gmail.com and Username: Marieka38187058;
- mariasmith12122@gmail.com and Username: AxlDeen;
- phone number 2035204961 and Username: FinnJaxen;
- phone number 2035204961 and Username: LilySlos; and
- phone number 2035204961 and Whateve18718239;

that are stored at premises owned, maintained, controlled, or operated by Twitter, Inc., a business with offices located at 1355 Market Street, Suite 900, San Francisco, California 94103.

ATTACHMENT A2

ITEMS TO BE SEARCHED

Associated files of Cybertipline Reports 90692565, 90693502, 90693602, and 90693794 that were forwarded to the National Center for Missing and Exploited Children (NCMEC) by Twitter, Inc.

ATTACHMENT B1 - Twitter, Inc.

I. Files and Accounts to be produced by Twitter, Inc., between September 11, 2018, to the present.

To the extent that the information described in Attachment A1 is within the possession, custody, or control of Twitter, Inc., including any messages, records, files, logs, images, videos, or information that have been deleted but are still available to Twitters, Inc., or have been preserved pursuant to the **preservation request made on May 11, 2021, and assigned case #s 0209428133**, Twitter, Inc. is required to disclose the following information to the government for each account or identifier listed in Attachment A1:

- a. All records or other information stored by an individual using the account, including address books, contact and friend lists, calendar data, pictures, videos, writings and files;
- b. All records or other information regarding the identification of the accounts described in A, to include full name, date of birth, gender, user name, vanity name, physical address, telephone numbers, email addresses and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, all screen names associated with subscribers and/or accounts, all account names associated with the subscriber, methods of connecting, log files, means and source of payment (including any credit or bank account number), and detailed billing records;
- c. Logs of tweets sent and received and for any unopened communication saved by a sender or recipient. Include the meta-data about the tweets;
- d. All Tweet and retweet content to include all images, videos and other files, to include deleted tweets and retweets, and associated sent date and timestamp, including all available metadata concerning these files;
- e. All direct messages sent and received, to include links, images, videos, deleted direct messages, and other files and messages and associated sent date and timestamp, including all available metadata concerning these messages;
- f. All pictures, memes, gifs, videos, files, links, tweets, messages, and other files stored, saved, sent, and received within accounts, to include deleted files, and associated sent date and timestamp, including all available metadata concerning these files;
- g. Payment information, including billing address, shipping address, and payment instruments, associated with any Twitter, Inc. services used by the accounts listed in Attachment A1;
- h. All information associated with the following Cybertipline reports: 90692565, 90693502, 90693602, and 90693794.

II. Information to be Seized by Law Enforcement Personnel

a. Any and all records that relate in any way to the email accounts described in Attachment A1 which is evidence, fruits, and instrumentalities of violations of Title 18 U.S.C. § 2251(a), 2252A(a)(2), 2252A(a)(5)(B), and 2261A(2)(b), specifically that relate to the following:

1. Images, videos and other files depicting the production, distribution, receipt, possession of or access with intent to view child erotica, child pornography, the sexual exploitation of minors, sexually explicit conduct, and illicit sexual conduct;
2. Communications or documentations regarding the production, distribution, receipt, possession of or access with intent to view child erotica, child pornography, the sexual exploitation of minors, sexually explicit conduct, and illicit sexual conduct;
3. Communication or documentation regarding access to and/or interaction with minors, to include the enticement of a minor;
4. Images depicting the interior or exterior of residences, public establishments, and vehicles;
5. All images, messages, communications, calendar entries, and contacts, including any and all preparatory steps taken in furtherance of these crimes;
6. Communication, information, documentation and records relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts;
7. Evidence of the times the account or identifier listed on Attachment A1 was used;
8. All images, messages and communications regarding wiping software, encryption or other methods to avoid detection by law enforcement;
9. Passwords and encryption keys, and other access information that may be necessary to access the account or identifier listed on Attachment A1 and other associated accounts;
10. Credit card and other financial information, including but not limited to, bills and payment records evidencing ownership of the subject account;

b. All existing printouts from original storage which concern the categories identified in subsection II.A; and

c. All "address books" or other lists of contact.

With respect to the search of the information provided pursuant to this warrant, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate

and expose those categories of files, documents, communications, or other electronically stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable.

If the government identifies any seized communications that may implicate the attorney-client privilege, law enforcement personnel will discontinue its review and take appropriate steps to segregate all potentially privileged information so as to protect it from substantive review. The investigative team will take no further steps regarding any review of information so segregated absent further order of the court. The investigative team may continue to review any information not segregated as potentially privileged.

ATTACHMENT B2

LIST OF ITEMS TO BE SEIZED

Any and all files containing a visual depiction of a minor, to include images and videos of children engaged in sexually explicit conduct as described in 18 U.S.C. § 2256, nude pictures, and modeling. Communication, information, pictures, videos or documentation that identifies the user of the account, that indicate a sexual interest in children, that indicates payment information, or that discuss the selling or purchasing of images and videos of children engaged in sexually explicit conduct.